(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 March 2002 (07.03.2002)

PCT

(10) International Publication Number
WO 02/19661 A3

(51) International Patent Classification[7]: H04L 29/06, 12/56

(21) International Application Number: PCT/US01/41961

(22) International Filing Date: 30 August 2001 (30.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/653,045 1 September 2000 (01.09.2000) US

(71) Applicant: TOP LAYER NETWORKS, INC. [US/US]; 2400 Computer Drive, Westboro, MA 01581-1770 (US).

(72) Inventors: NARAYANASWAMY, Krishna; c/o Top Layer Networks, Inc., 2400 Computer Drive, Westboro, MA 01581-1770 (US). SPINNEY, Barry, A.; c/o Top Layer Networks, Inc., 2400 Computer Drive, Westboro, MA 01581-1770 (US). ROSS, Theodore, L.; c/o Top Layer Networks, Inc., 2400 Computer Drive, Westboro, MA 01581-1770 (US). PAQUETTE, Michael, D.; Top Layer Networks, Inc., 2400 Computer Drive, Westboro, MA 01581-1770 (US). WRIGHT, Christopher, L.; Top Layer Networks, Inc., 2400 Computer Drive, Westboro, MA 01581-1770 (US).

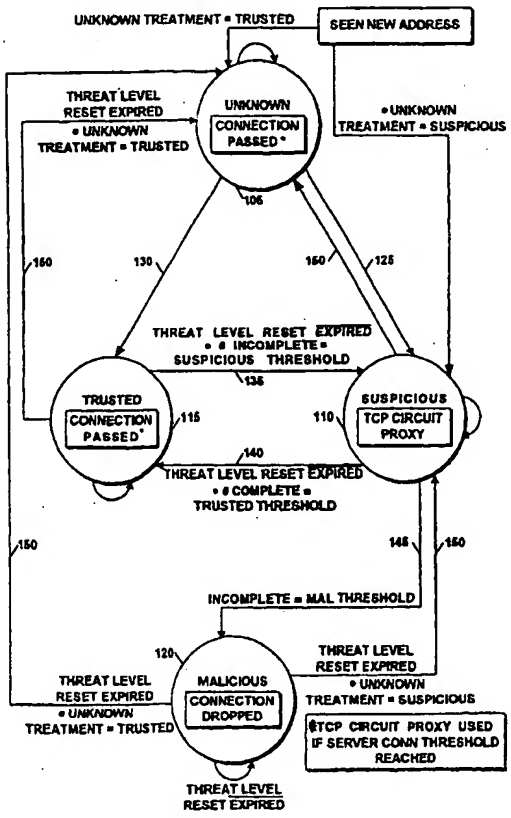
(74) Agents: CHOW, Stephen, Y. et al.; Perkins, Smith & Cohen, LLP, One Beacon Street, Boston, MA 02108 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian

*[Continued on next page]*

(54) Title: SYSTEM AND PROCESS FOR DEFENDING AGAINST DENIAL OF SERVICE ATTACKS ON NETWORK NODES




(57) Abstract: The present invention is a network switch that maintains a relatively lightly loaded state, and at the same time protects the network servers from DOS and DDOS attacks. The switch maintains a very large table of IP addresses where it stores information such as the number of incompleted and completed connections from each address. Using this information, the switch classifies each address into a threat level: unknown, trusted, suspicious, and malicious. Each threat level is treated differently allowing the switch to provide efficient access to the server while maintaining security. Connection to the server is denied to clients classified as malicious while trusted clients are passed through to the server. Suspicious connections are proxied while unknown connection treatment may be set by the user.

WO 02/19661 A3

patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

**(88) Date of publication of the international search report:**
18 April 2002

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/41961

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | WO 99 48303 A (CISCO TECH IND)<br>23 September 1999 (1999-09-23)<br>abstract; figures 4,2 | 1,3,6,<br>8-10 |
| A | page 2, line 31 -page 3, line 22<br>page 7, line 21 -page 9, line 17 | 2,4,5 |
| | --- | |
| X | SCHUBA C L ET AL: "Analysis of a denial of service attack on TCP"<br>SECURITY AND PRIVACY, 1997. PROCEEDINGS., 1997 IEEE SYMPOSIUM ON OAKLAND, CA, USA 4-7 MAY 1997, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US,<br>4 May 1997 (1997-05-04), pages 208-223, XP010230160<br>ISBN: 0-8186-7828-3<br>abstract<br>paragraphs '0004!,'0005! | 6-9 |
| | --- | |
| | -/-- | |

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance

'E' earlier document but published on or after the international filing date

'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

'O' document referring to an oral disclosure, use, exhibition or other means

'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

'&' document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 13 February 2002 | 19/02/2002 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Figiel, B |

1

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 01/41961

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| WO 9948303 A | 23-09-1999 | AU 3098299 A | 11-10-1999 |
| | | WO 9948303 A2 | 23-09-1999 |
| US 5958053 A | 28-09-1999 | EP 0956685 A1 | 17-11-1999 |
| | | WO 9834384 A1 | 06-08-1998 |